REQUEST FOR OFFER (RFO)
11-409.00-017

Information Technology Security Assessment and Security Plan

Date: April 24, 2012

You are invited to respond to this California Multiple Award Schedule (CMAS) Request for Offer (RFO) to provide Information Technology (IT) Security Consulting Services to the California Energy Commission (Energy Commission).

These services are needed to produce a written IT Security Assessment and Security Plan based on vulnerability testing and a security assessment of the Energy Commission's IT environment. The IT environment includes the IT infrastructure and the practices used to create, deliver, operate, secure, maintain and support the IT infrastructure. The services required are described in detail in the following Scope of Work (SOW). By submitting an offer, your firm agrees to the terms and conditions stated in this RFO and your proposed CMAS contract. Selection will be based on best value using the criteria listed in this document.

Please read this document carefully. All questions must be submitted via BidSync. Answers will be posted directly to the questions on BidSync. The RFO response including supporting documents, if any, as well as one (1) copy of the complete CMAS contract including the associated price list is due at **12 noon (PDT), Thursday, May 10, 2012.** Offers may be submitted electronically as long as it is smaller than 50 MB by the due date (and time) to Linda.Hoffman@energy.ca.gov. Multiple e-mails are acceptable to accommodate size limitation. If the response is mailed (including but not limited to U. S. Postal Service or overnight services) or hand delivered it must include one original and three copies as well as one (1) copy of the complete CMAS contract including the associated price list and be received by **12 noon (PDT), Thursday, May 10, 2012**. Any questions regarding this RFO should be directed to Ms. Hoffman.

Linda Hoffman
1516 9th Street, MS-7
Sacramento, CA 95814-5512
(916) 651-6179
Linda.Hoffman@energy.ca.gov

Table 1 provides the Key Dates concerning activities related to this RFO.

Table 1: Key RFO Dates

Release of RFO	Tuesday, April 24, 2012
Questions Due	Monday, April 30, 2012, 12 noon (PDT)
State Responses to Questions	Tuesday, May 1, 2012
RFO Response Due Date	Thursday, May 10, 2012, 12 noon (PDT),
Anticipated Contract Award	Thursday, June 14, 2012

Table of Contents

OVERVIEW

The Information Technology Services Branch (ITSB) within the Energy Commission seeks a Contractor to provide individuals, referred to as Consultants, with sufficient experience capable of undertaking all work assignments identified in the attached SOW. The Contractor and Consultants will receive assignments from and report to the Energy Commission Contract Manager (Contract Manager) and Energy Commission Project Manager (Project Manager).

The Energy Commission will only consider responses from Contractors with current contracts issued under the California Multiple Award Schedule (CMAS). The contract award, if made, will be under the terms of the existing agreement with the State for the selected Contractor and will be awarded to the Contractor submitting a response determined to provide the best value offer.

Pursuant to GC 19130 (b) (3): The services contracted are not available within civil service, cannot be performed satisfactorily by civil service employees, or are of such a highly specialized or technical nature that the necessary expert knowledge, experience, and ability are not available through the civil service system.

- **The maximum amount of this contract is $200,000.**
- **The start date is estimated to be June 18, 2012.**
- **The work requested under this contract must be completed by March 31, 2014.**

BACKGROUND

The Energy Commission is the state's primary energy policy and planning agency. An overview of the Energy Commission can be viewed at the Energy Commission’s home page – http://www.energy.ca.gov. Created by the Legislature in 1974 and located in Sacramento, the Energy Commission has five major responsibilities:

- Forecasting future energy needs and keeping historical energy data.
- Licensing thermal power plants 50 megawatts or larger.
- Promoting energy efficiency through appliance and building standards.
- Developing energy technologies and supporting renewable energy.
- Planning for and directing state response to energy emergency.

ITSB is the custodian of the IT environment which is necessary to facilitate the business needs of the Energy Commission’s mission.

ITSB technical and security staff are actively involved in providing adequate security measures for the Energy Commission’s IT environment. Over the years, several policies, standards, processes and procedures surrounding IT security have been developed.

Government Code, Section 11546.3, created by AB 2408 (Chapter 404, Statutes of 2010), requires the Energy Commission to modify and expand its IT infrastructure. These include expanding its network, moving critical infrastructure to a new data center, and integrating into the new data center's shared services.

These changes will require ITSB technical and security staff to grow in their knowledge and expertise in order to continue to implement the necessary security measures to protect the Energy Commission's IT environment. The ensuing results from the vulnerability testing and security assessment will provide the necessary direction to ITSB management, technical, and security staff to ensure a realistic response to current threats and risks to the Energy Commission's IT environment.

PROJECT INFORMATION

The Energy Commission's ITSB is seeking an IT Security Contractor to do the following:

- Perform Vulnerability Testing. Vulnerability testing (or penetration testing) will be used to analyze the Energy Commission's IT environment for any potential vulnerabilities that could be the result of poor or improper system configuration, both known and unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures.
- Perform an IT Security Assessment. The security assessment will include an evaluation of the security technologies and practices currently in place, a review of the Energy Commission's security and information management policies, procedures, and practices, and an identification of gaps where additional measures should be taken.
- Produce a written IT Security Assessment and Security Plan. The IT Security Assessment and Security Plan will be a final report of all the findings and results from the vulnerability testing and security assessment and will include a prioritized plan of action. The prioritized plan of action will include recommended improvements with an estimated schedule and costs.
- Assist with the initial implementation of quick wins and priority recommended improvements identified in the IT Security Assessment and Security Plan.

For more details about the work to be done and the deliverables, please see the Scope of Work section of this document.

RFO RESPONSES

Reponses to this RFO must include a complete copy of the CMAS contract, including the price list the response is based on, and must be received no later than 12 noon (PDT) on Thursday, May 10, 2012. To expedite this process clarification questions must be submitted via BidSync no later than 12 noon on Monday, April 30, 2012. To create a question on BidSync, go to the RFO page, approximately 4 lines below the title bar click on "View Questions & Answers," then click the "Create New Question" button on the right side of the page. Responses to the questions will be posted on the RFO page at BidSync by 4:00 p.m. (PDT) on Tuesday, May 1, 2012.

Responses must include three (3) references for the Contractor and resumes and three (3) references for each Consultant. Please use the forms in Attachment A. Interviews and reference checks will be at the discretion of the Energy Commission. To clarify terminology, the Contractor is the responding firm or company, while the Consultant is any specific individual who will perform the work. If the Consultant is also the Contractor, the Consultant’s references may also be used as the Contractor references.

SELECTION CRITERIA

The following chart lists how received offers will be compared:

	Item	Section Total	Individual Item
1	Completeness	Pass/Fail	
	□ Offers received as required; date/time □ Contractor References (3) □ Consultant References (3) □ Consultant Resumes □ CMAS Contract and price list □ Consultant classifications and hourly rates		Responses must “Pass” to be eligible for further evaluation
2	Experience		
	CONTACTOR EXPERIENCE (Qualitative)	25	
	□ Background – brief profile of the company’s past successful projects similar to this RFO. Please include work projects the company was involved in that were of similar type, size/scope, and complexity. An ideal response should show a history of at least three years, and most recent project should be within the past two years.		15
	□ Example of completed IT Security Assessment and Security Plan.		10
	CONSULTANT EXPERIENCE	35	
	□ Lead Consultant: Certification in an industry-recognized certification in information security, such as Certified Information Systems Security Professional (CISSP), or Certified Information Systems Auditor (CISA) (1 point per year to a maximum of 15 points).		15
	□ Experience conducting vulnerability testing and IT security assessments (1 point per year to a maximum of 10 points)		10
	□ Experience with California state government performing IT security consulting and assisting with IT security assessments and planning (1 point per year of experience to a maximum of 10 points)		10

3	Quality of Proposal Response	20	
	□ Content of proposal response (completeness of the response in addressing the RFO, clear understanding of the work being solicited)		15
	□ Technical quality of proposal response (e.g., overall organization, grammar, presentation, professionalism, clear ability to communicate)		5
4	Cost	10	
	□ Cost – See Cost Evaluation below		10
5	References	10	
	□ Evaluation of References – Calls will only be made if the sub-total for selection criteria 2 through 4 is within 20 points of the highest score.		10

COST EVALUATION

It is anticipated that all offers will come in at or near the total of $100,000; the cost evaluation will be based on Consultant's hourly rates. If the offer includes more than one Consultant, the cost evaluation will be based on the Consultants' average hourly rates.

Cost evaluation will be based as follows:

$$\frac{\text{Lowest Received Offer}}{\text{Contractor's Offer}} \quad \text{X} \quad \text{Maximum Cost Score} \quad = \quad \text{Cost Score}$$

Resource	Contractor #1	Contractor #2	Contractor #3
Contractor Offer	$93,000	$97,000	$100,000
	$\frac{93K}{93K}$ X 10 = 10	$\frac{93K}{97K}$ X 10 = 9.6	$\frac{93K}{100K}$ X 10 = 9.3

SCOPE OF WORK

Task Number	Description
1	Status Reports & Meetings
2	Project Planning
3	Information Gathering
4	Vulnerability Testing
5	IT Security Assessment
6	IT Security Assessment and Security Plan
7	Initial Implementation of the IT Security Assessment and Security Plan
---	Unanticipated Tasks
---	Key Deliverables and Estimated Deadlines
---	Acceptance Criteria
---	Additional Contract Terms

Task 1 – Meetings & Status Reports

Description

The Contractor will attend regularly scheduled meetings. These meetings will include but not be limited to:

1. An initial kick-off meeting at the beginning of the project.
2. Project planning and status meetings.
3. Information gathering meetings and interviews.
4. Final presentation meeting.

In addition, the Contractor will provide regularly scheduled status reports. The status reports will include but not be limited to:

1. Current status on the overall progress of the project.
2. Percentage of milestones completed.
3. Identified issues/risks and mitigation steps.
4. Contract administration items including budget and invoice questions.

Deliverables

□ Attend meetings.
□ Status reports.

Task 2 – Project Planning

Description

The Contractor, in cooperation with the Project Manager, will create and maintain a Project Plan using Microsoft Project. The Project Plan should provide a list of tasks, the timeframe for each task, the dependencies between them and the resources needed.

The project plan will be used as a communication tool to communicate the responsibilities of the Contractor, Consultants, and Energy Commission staff.

Deliverables

- Project plan with project tasks, timelines, dependencies and resources.
- Updates to the project plan as adjustments are identified.

Task 3 – Information Gathering

Description

The Contractor will gather as much information as possible about the Energy Commission’s IT environment.

The information gathering will include but not be limited to:

1. All documentation relating to IT security policies, standards, processes and procedures.
2. All IT infrastructure diagrams, drawings, spreadsheets, lists, inventories and other documents.
3. Any documentation relating to currently implemented security technologies.
4. Any pre-existing analyses of the Energy Commission’s IT environment.
5. Any pertinent monitoring logs or other similar documentation.

In addition, the Contractor will conduct group meetings and individual interviews with staff to gather additional information about the Energy Commission’s IT environment.

The Contractor will be expected to compile and summarize all information gathered. This information will be used as a baseline for the IT Security Assessment in Task 5.

Deliverables

- A compilation and list of all documents gathered.
- The completion of all interviews and documentation of the interview findings.

Task 4 – Vulnerability Testing

Description

The Contractor will perform vulnerability testing using pre-approved tools and processes to scan the Energy Commission’s existing IT infrastructure for vulnerabilities. In preparation of the vulnerability testing the Contractor will review the proposed tools and processes with Energy Commission ITSB technical staff and management. This approval process will be use to evaluate any potential risks to the Energy Commission that may be associated with the proposed tools and processes. Upon approval the vulnerability testing may begin.

The vulnerability testing should include a scan of specific targets and may include firewalls, routers, switches, appliances, and servers. The Contractor will work with ITSB technical staff and management to define the specific targets to test. The identified targets will be documented and the testing dates will be incorporated into the project plan.

In addition, the vulnerability testing may be used as a training opportunity for ITSB staff whereby the Contractor will provide instruction on the tools and processes.

Upon completing the vulnerability testing, the Contractor will analyze all information derived from the testing procedures. The analysis will be used to uncover security weaknesses and to expose vulnerabilities of the tested systems. The Contractor will list and prioritize vulnerabilities and categorize risks as high, medium, or low and recommend repairs if vulnerabilities are found.

Deliverables

- Conduct vulnerability testing on the approved targets.
- Train up to five ITSB technical staff on the vulnerability testing tools and processes.
- Perform an analysis of the data and produce reports from the data including:
  - An executive summary summarizing the vulnerability testing findings.
  - A technically detailed report of the findings listing information about each device's vulnerabilities.
  - Additional information, such as raw scanner output, Whois records, screenshots, diagrams, and relevant white papers may be included as an appendix of the IT Security Assessment and Security Plan Report in Task 6.

Task 5 – IT Security Assessment

Description

The Contractor will conduct an IT Security Assessment of the Energy Commission's IT environment and provide a gap analysis identifying the gaps between the Energy Commission's current IT environment and industry (ANSI, ISO), state (SAM, SIMM) and federal (NIST, FIPS) policies, standards and requirements.

The IT Security Assessment will include but not be limited to:

1. Review applicable State, Federal and industry information security policies, standards to identify requirements as they relate to data confidentiality, privacy and security.
2. Assess current network security measures as they compare to security best practices, business objectives, and regulatory requirements.
3. Review of physical and logical access controls and mechanisms.
4. Review of system monitoring and auditing practices, including what records and logs are produced, what audit procedures and practices are employed, and what follow-up procedures are adopted.
5. Review of practices, procedures and risks with respect to hardware and hardware maintenance.
6. Review of change control procedures and practices, both scheduled and emergency.
7. Review of security administration practices in regard to resource access, system access and security system control.
8. Review of contingency and recovery plans.

9. Review of existing IT security policies, guidelines, and standards.
10. Review of IT security awareness policies and practices.

Deliverables

- A review of the Energy Commission’s IT environment.
- A draft of the IT Security Assessment findings and gap analysis.
- A final copy of the IT Security Assessment findings and gap analysis that incorporates any feedback from Energy Commission staff to be used in the IT Security Assessment and Security Plan as identified in Task 6.

Task 6 – IT Security Assessment and Security Plan

Description

The Contractor will produce a written IT Security Assessment and Security Plan based on the findings from the vulnerability testing and IT security assessment. The IT Security Assessment and Security Plan will provide a baseline of the current IT environment and a prioritized plan of action. The prioritized plan of action will include recommended improvements with an estimated schedule and costs.

The IT Security Assessment and Security Plan will include but not be limited to:

1. Introduction/background information.
2. Executive and Management summary.
3. IT security assessment scope and objectives.
4. Assumptions and limitations.
5. Methods and assessment tools used.
6. Current environment or system description with network diagrams, if any.
7. A summary of findings and recommendations.
8. The vulnerability testing results.
9. IT security assessment results including identified assets, threats, vulnerabilities, impact and likelihood assessment, and the risk results analysis.
10. A prioritized list of recommended improvements with an estimated cost for implementing each recommendation.
11. An estimated schedule for implementation of the recommendations.

Deliverables

- A draft IT Security Assessment and Security Plan for review by Energy Commission staff.
- A final IT Security Assessment and Security Plan that incorporates any feedback from Energy Commission staff.

Task 7 – Initial Implementation of the IT Security Assessment and Security Plan

Description

The Contractor will assist ITSB staff with the initial implementation of the IT Security Assessment and Security Plan.

The Contractor in coordination with the Project Manager will:

1. Prepare a list of quick wins and of priority recommendations from the IT Security Assessment and Security Plan.
2. Assess the list against the Contractors remaining budget and the costs associated with assisting with the implementation.
3. Determine a final list based on the Contractors remaining budget.
4. Update the Project Plan incorporating the final list with a timeline, dependences, and resource requirements.

Based on the updated Project Plan the Contractor will assist ITSB staff with the implementation of the identified quick wins and priority recommendations.

Deliverables

- Quick wins and priority recommendations list.
- Final list and updated Project Plan.
- Completion of agreed upon quick wins and priority recommendations.

Unanticipated Tasks

The State may add an additional amount in the contract for unanticipated tasks. Unanticipated tasks will be executed as change orders, in the event that additional work must be performed which was wholly unanticipated, and which was identified in neither the State’s solicitation document nor the Contactor’s bid submitted in response thereto, but which in the opinion of both parties is necessary to the successful accomplishment of the general scope of work.

Key Deliverables and Estimated Deadlines

Key Deliverable	Estimated Date
Kickoff Meeting: Within three weeks of award of purchase order.	**July 2, 2012**
Delivery of Initial Project Plan: Within one week following the Kickoff Meeting.	**July 9, 2012**
Delivery of Information Gathering findings and documentation: Within two weeks of approval of initial project plan.	**July 23, 2012**
Delivery of Vulnerability Testing results and analysis: Within six weeks of approval of initial project plan.	**Aug 20, 2012**
Delivery of IT Security Assessment findings and gap analysis: Within three weeks of completion of the Vulnerability Testing.	**Sept 10, 2012**
Delivery of Final IT Security Assessment & Security Plan: Within four weeks of completion of the IT Security Assessment.	**Oct 8, 2012**
Implementation of Quick Wins & Priority Recommendations: Within six months of completion of the IT Security Assessment.	**Mar 31, 2012**

Acceptance Criteria

Energy Commission staff will be the sole judge of the completion and acceptability of the final state of all key deliverables produced by the Contractor.

Acceptance criteria consist of the following:

1. All key deliverables must be complete and comprehensive incorporating all feedback received from staff review and of a level of quality acceptable to the Energy Commission.
2. The Project Manager must approve the format and content of all key deliverables in advance.
3. All deliverables must be completed, as specified, and approved by the Project Manager in writing.

If a deliverable is not acceptable, the Project Manager will provide the reason, in writing, within five (5) working days of receipt of the deliverable.

Additional Contract Terms

The contract is subject to the CMAS terms and conditions between the Contractor and the State of California, except as specified below:

1. This is a fixed-price, deliverables contract. All costs must be inclusive of labor and other direct costs, including travel.
2. Progress payments will be made upon written acceptance of the key deliverables. Itemized invoices must include the RFO number and submitted in triplicate to:

   California Energy Commission
   Attn: Accounting Office
   1516 9th Street, MS -
   Sacramento, CA 95814

3. Payment withholding will apply. Ten percent (10%) of the invoiced amount will be withheld pending final completion, receipt, and acceptance by the Energy Commission of the final key deliverable.
4. The Final Invoice will be considered acceptable when the Energy Commission determines that the invoices for this contract accurately account for all work performed on the contract without any internal inconsistencies, discrepancies, or unbilled periods. Any inconsistencies or omissions present in any invoices must be corrected before the final invoice will be considered acceptable.

ATTACHMENT A: REFERENCE FORM

Please complete three (3) reference forms for the Contractor and each Consultant.

REFERENCE #			
1. Contractor or Consultant Info			
Name:	Primary Contact Phone Number:		
Reference is for: □Contractor □Consultant □Both (if same)			
2. Client info			
Client Name:	Contact Name:		
Address:	Contact Phone:		
3. Project/ Work info			
Name of Project:	Dates Served on Project (from/to):		
Project Description:			
Contractor or Consultant Involvement on the Project:			
Deliverables Prepared By Contractor or Consultant:			
4. Project Measurements and Results			
Original estimated hours on project:	Actual hours on project:		
		YES	NO
Was the project or contract terminated prior to successful conclusion? If “yes,” please explain the reason.			
Were your work products reviewed and approved by any agency outside the client? If “yes”, please list the approving agencies.			